Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. (currently amended) A security processing method comprising:

receiving, by a security processor, an internal outbound packet from an Ethernet controller over a network, wherein the internal outbound packet includes a flow identifier for the internal outbound packet and security processor address data;

processing at least a portion of the received internal outbound packet if the security processor address data matches address information ~~associated with~~ assigned to the security processor, wherein the processing includes:

using the flow identifier as a direct address handle to retrieve a security association for the received internal outbound packet,

performing a cryptographic operation on a portion of the received internal outbound packet using at least a portion of the retrieved security association, and

assembling an outbound network packet including a header and the cryptographically processed portion of the received internal outbound packet; and

transmitting, from the security processor, the outbound network packet to an external network.

2. (previously presented) The method of claim 1 wherein performing the cryptographic operation comprises performing one or more IPsec operations.

3. (original) The method of claim 2 wherein the IPsec operations comprise adding or removing protocol elements.

4-6. (canceled)

7. (previously presented) The method of claim 1 wherein the security processor resides on a network interface card (NIC).

8. (currently amended) A security processor comprising:

at least one media access controller (MAC); and

at least one processor configured to:

receive an internal outbound packet from an Ethernet controller via the at least one MAC, wherein the internal outbound packet includes a flow identifier for the internal outbound packet and security processor address data,

process at least a portion of the received internal outbound packet if the security processor address data matches address information ~~associated with~~ assigned to the security processor, including:

using the flow identifier as a direct address handle to retrieve a security association for the received internal outbound packet,

performing a cryptographic operation on a portion of the received internal outbound packet using at least a portion of the retrieved security association, and

assembling an outbound network packet including a header and the cryptographically processed portion of the received internal outbound packet; and

transmitting the outbound network packet from the security processor to an external network.

9. (original) The security processor of claim 8 wherein the at least one processor comprises at least one IPsec processor.

10. (previously presented) The security processor of claim 9 wherein the IPsec processor is configured to add IPsec protocol elements to or to remove IPsec protocol elements from the internal outbound packet or the outbound network packet.

11. (canceled).

12. (previously presented) The security processor of claim 8 further comprising at least one data memory for storing security association information for use by the at least one processor, wherein the security association information includes a handle and security association data.

13-14. (canceled).

15. (previously presented) The security processor of claim 8 wherein the security processor resides on a network interface card (NIC).

16. (currently amended) An in-line security processor comprising:

a plurality of media access controllers (MACs); and

at least one processor configured to receive an internal outbound packet from an Ethernet controller via at least one of the plurality of MACs, wherein the internal outbound packet includes a flow identifier for the internal outbound packet and security processor address data,

process at least a portion of the received internal outbound packet if the security processor address data matches address information ~~associated with~~ assigned to the security processor, including:

using the flow identifier as a direct address handle to retrieve a security association for the received internal outbound packet,

performing a cryptographic operation on a portion of the received internal outbound packet using at least a portion of the retrieved security association, and

assembling an outbound network packet including a header and the cryptographically processed portion of the received internal outbound packet; and

transmitting the outbound network packet from the in-line security processor to an external network.

17. (original) The in-line security processor of claim 16 wherein the at least one processor comprises at least one IPsec processor.

18. (previously presented) The in-line security processor of claim 17 wherein the IPsec processor is configured to add IPsec protocol elements to or to

remove IPsec protocol elements from the internal outbound packet or the outbound network packet.

19. (canceled).

20. (original) The in-line security processor of claim 16 further comprising at least one data memory for storing security association information for use by the at least one processor.

21. (currently amended) A security processing system comprising:

at least one media access controller (MAC);

at least one security processor configured to:

receive an internal outbound packet from an Ethernet controller via at least one MAC, wherein the internal outbound packet includes a flow identifier for the internal outbound packet and security processor address data,

process at least a portion of the received internal outbound packet if the security processor address data matches address information ~~associated with~~ assigned to the at least one security processor, including:

using the flow identifier as a direct address handle to retrieve a security association for the received internal outbound packet,

performing a cryptographic operation on a portion of the received internal outbound packet using at least a portion of the retrieved security association, and

assembling an outbound network packet including a header and the cryptographically processed portion of the received internal outbound packet; and

at least one switch between the at least one media access controller and the at least one security processor; and

transmitting the outbound network packet from the at least one security processor to an external network.

22. (original) The security processing system of claim 21 wherein the at least one media access controller comprises at least one Gigabit MAC.

23. (previously presented) The security processing system of claim 21 wherein the at least one security processor is further configured to allocate memory space associated with the security association used by the at least one security processor.

24. (original) The security processing system of claim 21 wherein the at least one switch associates VLAN tags with the at least one media access controller.

25-26. (canceled)

27. (currently amended) A chassis-based switch comprising:

at least one backplane;

at least one processing blade connected to the at least one backplane, the at least one processing blade comprising at least one media access controller; and

at least one switching blade connected to the at least one backplane, the at least one switching blade comprising:

at least one security processor configured to:

receive an internal outbound packet from an Ethernet controller, wherein the internal outbound packet includes a flow identifier for the internal outbound packet and security processor address data,

process at least a portion of the received internal outbound packet if the security processor address data matches address information ~~associated with~~ assigned to the at least one security processor, including:

using the flow identifier as a direct address handle to retrieve a security association for the received internal outbound packet,

performing a cryptographic operation on a portion of the received internal outbound packet using at least a portion of the retrieved security association, and

assembling an outbound network packet including a header and the cryptographically processed portion of the received internal outbound packet; and

at least one packet switch between the at least one media access controller and the at least one security processor; and

transmitting the outbound network packet from the at least one security processor to an external network.

28-32. (canceled)

33. (currently amended) A security processing system comprising:

at least one Ethernet controller configured to:

receive a TCP/IP packet in a data flow and store context information associated with the TCP/IP packet;

identify flow identification information for the data flow including a flow identifier; and

generate an internal outbound packet including a security identifier header having the flow identifier, security processor address data, and at least a portion of the TCP/IP packet; and

at least one security processor configured to:

receive the internal outbound packet from the at least one Ethernet controller, wherein the internal outbound packet includes a flow identifier for the packet and security processor address data,

process at least a portion of the received internal outbound packet if the security processor address data matches address information ~~associated with~~ assigned to the security processor, including:

using the flow identifier as a direct address handle to retrieve a security association for the received internal outbound packet,

performing a cryptographic operation on a portion of the received packet using at least a portion of the retrieved security association, and

assembling an outbound network packet including a header and the cryptographically processed portion of the received internal outbound packet; and

transmitting the outbound network packet from the at least one security processor to an external network.

34. (withdrawn) A method of configuring a security processor comprising:

generating configuration information;

formatting the configuration information into at least one packet; and

sending the at least one packet over a Gigabit Ethernet network to a security processor.

35. (withdrawn) The method of claim 34 wherein the at least one packet comprises at least one IPsec packet.

36. (withdrawn) A method of configuring a security processor comprising:

receiving at least one packet containing configuration information over a Gigabit Ethernet network;

extracting the configuration information from the at least one packet; and

configuring a security processor using the extracted configuration information.

37. (withdrawn) The method of claim 36 wherein the at least one packet comprises at least one IPsec packet.

38. (withdrawn) A method of configuring a security processor comprising:

generating at least one security association;

formatting the at least one security association into at least one packet; and

sending the at least one packet over a Gigabit Ethernet network to a security processor.

39. (withdrawn) A method of configuring a security processor comprising:

receiving at least one packet containing at least one security association over a Gigabit Ethernet network; extracting the at least one security association from the at least one packet; and

storing the extracted at least one security association.

40-50. (canceled).

51. (previously presented) The security processing system of claim 33 wherein the at least one security processor is further configured to modify at least one checksum in the security identifier header.

52. (previously presented) The security processing system of claim 33 wherein the at least one Ethernet controller modifies at least one maximum transmitted unit size in accordance with modifications the at least one security processor makes to at least a portion of the outbound network packets.

53. (previously presented) The security processing system of claim 33 wherein the at least one Ethernet controller reduces at least one TCP/IP payload size in accordance with at least one security header and trailer size added to at least a portion of the outbound network packets.

54 - 55 (canceled).

56. (previously presented) The security processing system of claim 33 wherein the at least one Ethernet controller securely communicates with the at least one security processor to configure the at least one security processor or retrieve status information from the at least one security processor.

57. (canceled).

58. (previously presented) The method of claim 1, further comprising:

entering a low power state upon receipt of a low-power configuration signal, wherein entering the low power state includes:

disabling an IPSec data path and a public key data path.

59. (previously presented) The method of claim 58, further comprising:

receiving a second configuration signal indicating a release from low power state; and

enabling the IPSec data path and the public key data path.

60. (previously presented) The method of claim 1, further comprising:

prior to receiving the internal outbound packet in a flow,

receiving security association information for the flow, the security association information including a security association handle and security association data.

61. (previously presented) The method of claim 60, further comprising:

storing the security association information in a local memory associated with the security processor.

62. (previously presented) The method of claim 1, wherein the security processor resides on a motherboard of a computer system.

63. (previously presented) The security processor of claim 8, wherein the at least one processor is further configured to enter a low power state upon receipt of a low-power configuration signal and disable an IPSec data path and a public key data path.

64. (previously presented) The security processor of claim 63, wherein the at least one processor is further configured to:

receive a second configuration signal indicating a release from low power state; and

enable the IPSec data path and the public key data path.

65. (previously presented) The security processor of claim 8, wherein the at least one processor is further configured to receive security association information for the flow, the security association information including a security association handle and security association data.

66. (previously presented) The security processor of claim 65, wherein the at least one processor is further configured to store the security association information in a local memory associated with the security processor.

67. (previously presented) The security processor of claim 8, wherein the security processor resides on a motherboard of a computer system.

68. (previously presented) The security processor of claim 8, wherein the security processor is in-line with a data path of a packet network.